PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-239125
(43)Date of publication of application : 31.08.1999

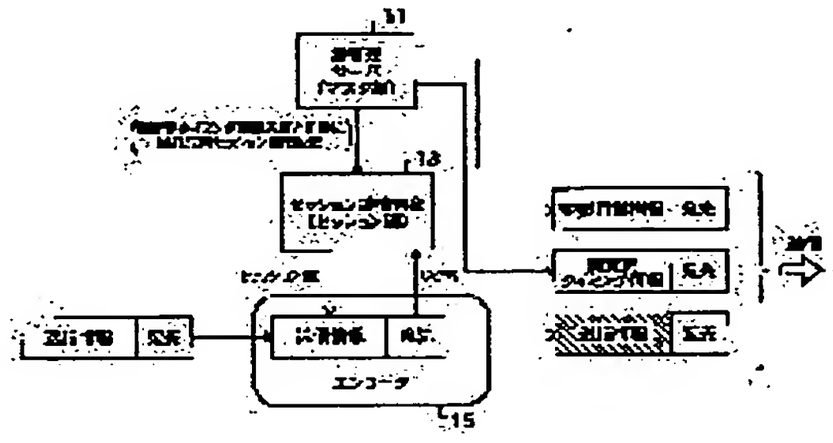
(51)Int.CI. H04L 9/08

(21)Application number : 10-040641
(22)Date of filing : 23.02.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KAWABATA MICHIO
NIHEI KATSUTOSHI
NAKAYAMA MASAYOSHI
ARAKI KATSUHIKO

(54) METHOD AND SYSTEM FOR CRYPTOGRAPHIC COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To remarkably increase the number of session keys and master keys handleable at an information transmission station by reducing the number of pieces of key information for change by transmitting the session key, which is enciphered by each master key for destination, just for plural destinations.
SOLUTION: When changing the session key, first of all, the destination is turned into destination to change the session key by a key managing server 11 at the information transmission station, a newly generated session key is enciphered by the master key for session key distribution for each destination, and key information for change is generated and transmitted. Afterwards, key application timing information is generated for reporting the application timing of the new session key transmitted by the key information for change to an information reception station and the destination is transmitted as the destination to change the session key. Besides, together with the transmission of key change timing information, the session key for the relevant destination preserved in a session key retrieving part 13 is changed to the new session key.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－239125

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/08		H04L 9/00	601B
			601A
			601E

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－40641

(22)出願日　平成10年(1998)２月23日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　川畑　道朗
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　仁平　勝利
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　中山　正芳
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　三好　秀和　（外１名）

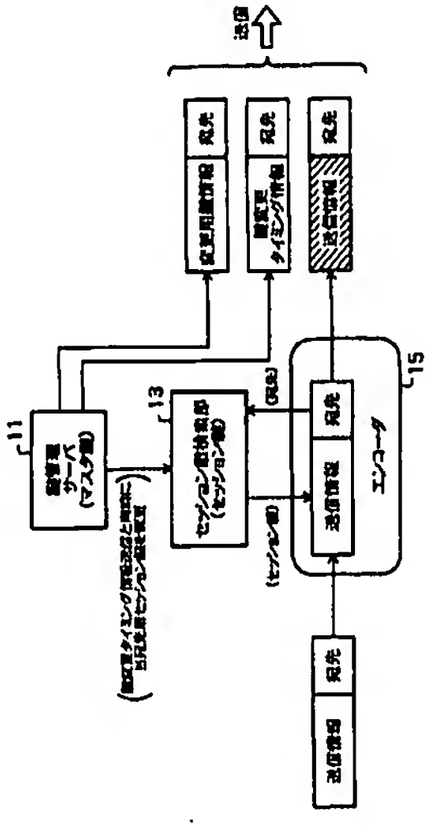
最終頁に続く

(54)【発明の名称】　暗号化通信方法および暗号化通信システム

(57)【要約】

【課題】　本発明は、番組単位のみならず受信局単位の暗号化を可能にすると共に、変更用鍵情報等の送信数を極力、小さくすることのできる暗号化通信方法および暗号化通信システムを提供することを目的とする。

【解決手段】　情報送信局は、全宛先用のセッション鍵およびマスタ鍵とを保持し、伝送情報を送信するときには当該伝送情報の宛先に対応するセッション鍵を用いて伝送情報を暗号化して送信し、前記セッション鍵を変更する際には変更用鍵情報に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信し、受信端末は、割り当てられる宛先用のセッション鍵と宛先用マスタ鍵とを保持し、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化し、前記セッション鍵を変更する際には前記変更用鍵情報を受信して前記記憶手段に記憶されるマスタ鍵を用いて復号して変更されたセッション鍵を得る。



1

【特許請求の範囲】

【請求項１】　情報送信局で暗号化され所定の宛先が付与された伝送情報を送信し、この伝送情報を当該宛先の受信端末で受信し復号化するときの暗号化通信方法であって、

情報送信局は、全宛先用のセッション鍵およびマスタ鍵とを記憶し、伝送情報を送信するときには当該伝送情報の宛先に対応するセッション鍵を用いて伝送情報を暗号化して送信し、

受信端末は、当該受信端末が受信資格のあるときに割り当てられる宛先用のセッション鍵と宛先用マスタ鍵とを記憶し、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化し、

前記セッション鍵を変更する際には、情報送信局は、この情報送信局より送信される変更用鍵情報に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信し、

受信端末は、前記変更用鍵情報を受信したときには前記受信端末に記憶されるマスタ鍵を用いて復号し、変更されたセッション鍵を得ることを特徴とする暗号化通信方法。

【請求項２】　前記変更用鍵情報は、各宛先用の鍵変更タイミング情報と共に送信され、当鍵変更タイミング情報に従って前記情報送信局および当該宛先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを特徴とする請求項１記載の暗号化通信方法。

【請求項３】　前記情報送信局は、変更用鍵情報及び鍵変更タイミング情報を複数回繰り返して送信することを特徴とする請求項１または２記載の暗号化通信方法。

【請求項４】　前記情報送信局は複数であることを特徴とする請求項１、２または３記載の暗号化通信方法。

【請求項５】　前記セッション鍵の変更は、変更周期が各宛先毎に変えて行われることを特徴とする請求項１乃至４のいずれかに記載の暗号化通信方法。

【請求項６】　情報送信局で暗号化され所定の宛先が付与された伝送情報を送信し、この伝送情報を当該宛先の受信端末で受信し復号化するときの暗号化通信システムであって、

情報送信局は、全宛先用のセッション鍵およびマスタ鍵とを記憶する記憶手段と、伝送情報を送信するときには当該伝送情報の宛先に対応するセッション鍵を用いて伝送情報を暗号化して送信する伝送情報暗号化手段と、前記セッション鍵を変更する際に変更用鍵情報に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信する変更用鍵情報暗号化手段とを有し、

受信端末は、当該受信端末が受信資格のあるときに割り当てられる宛先用のセッション鍵と宛先用マスタ鍵とを記憶する記憶手段と、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化する伝送情報復号化手段と、前記セッション鍵を変更する際に前記変更用鍵情報を受信して前記記憶手段に記憶されるマスタ鍵を用いて復号して変更されたセッション鍵を得る変更用鍵情報復号化手段と有することを特徴とする暗号化通信システム。

【請求項７】　前記変更用鍵情報は、各宛先用の鍵変更タイミング情報と共に送信され、当鍵変更タイミング情報に従って前記情報送信局および当該宛先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを特徴とする請求項６記載の暗号化通信システム。

【請求項８】　前記情報送信局は、変更用鍵情報及び鍵変更タイミング情報を複数回繰り返して送信することを特徴とする請求項６または７記載の暗号化通信システム。

【請求項９】　前記情報送信局は複数であることを特徴とする請求項６、７または８記載の暗号化通信システム。

【請求項１０】　前記セッション鍵の変更は、変更周期が各宛先毎に変えて行われることを特徴とする請求項６乃至９のいずれかに記載の暗号化通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報送信局から受信端末への通信を提供する通信システムにおける暗号化通信方法および暗号化通信システムに関するものである。

【０００２】

【従来の技術】近年、衛星放送が普及してきており、この衛星放送では有料放送の映像や音声等に対してスクランブルを施すことにより不正視聴を防ぐようにしてる。このような衛星放送で用いられているスクランブル方法の３重鍵暗号の概要を図１５に示す。

【０００３】図１５において、鍵Ｋｓは送信側の送信局と受信側のＢＳデコーダで正しく対応したスクランブル／デスクランブル処理を行うための鍵で、鍵Ｋｗは番組情報の暗号の鍵で、鍵ＫｍはＢＳ（Ｂｒｏａｄｃａｓｔｉｎｇ　ｓａｔｅｌｌｉｔｅ；放送衛星）デコーダ毎に固有の個別情報の暗号の鍵である。

【０００４】この図１５に示す方法では、ＢＳデコーダでは送信局と同じ擬似ランダムデータ列を発生し、映像・音声信号をデスクランブルすることになる。この擬似ランダムデータ列を発生するために、スクランブルの鍵Ｋｓが送られるが、鍵Ｋｓは番組情報の一部として暗号化されており、ＢＳデコーダではこれを解く鍵Ｋｗがないと暗号解読できない。さらに、鍵Ｋｗは個別情報の一部として暗号化されており、ＢＳデコーダ固有の鍵Ｋｍがないと暗号解読できない。さらに、この鍵Ｋｗを含んだ個別情報は、視聴料金を納めた視聴者だけに送信される。鍵ＫｍはＢＳデコーダ毎に異なるため、視聴料金未納者のＢＳデコーダでは暗号の復号ができず、鍵Ｋｗを

知ろうとしても不可能であり、不正視聴はできないようになっている。

【0005】この方法において、番組情報は鍵Ksなどのデスクランブルに必要な情報を担って約1秒に1回送信される。このため、BSデコーダが番組情報を取り落とすと、この直後約1秒は確実にデスクランブルできなくなってしまう。そこで同じ番組情報を複数回連続送信して受信側で多数決判定できるようにしている。

【0006】また、この方法で用いられるスクランブルアルゴリズムは、映像信号のライン毎に切れ目を入れ左右を入れ替えるラインローテーションや、映像信号のラインを入れ替えるラインパーミュテーションなどが用いられている。

【0007】また、CS（Communication satellite；通信衛星）デジタル放送では、上記の方法と同様に、鍵構成は3層で、暗号化はDVB（Digital Video Broadcasting）との共通化を図るため、MPEG2 Video&AudioおよびSystemsを骨格とした方式を採用している。このため、暗号化はMPEG2のトランスポートストリームという情報単位で行い、暗号化アルゴリズムは共通鍵暗号法の1つであるMulti2の鍵長32ビット以上の鍵を用いて行っている。この方法では、最大96種類のトランスポートストリームに対し異なる鍵を用いて暗号化を行うことができる。

【0008】また、ATM（Asynchronous Transfer Mode；非同期転送モード）を用いた片方向通信システムでのセッション鍵の変更法が「ATM Forum Technical Committee, Phase IATM Security Specification (Draft), September, 1997」に示されている。このセッション鍵変更法を以下に示す。

【0009】まず、セキュリティ向上のために行うセッション鍵の変更は、各番組用のマスタ鍵を各番組の受信資格を持つ全ての受信局に予め与えておく。

【0010】情報送信局でセッション鍵を変更する番組用の新しい鍵を生成し、生成した新しい鍵を当該番組用のマスタ鍵で暗号化しセッション鍵送信用のSKE OAM（Operation, Administration and Maintenance；運用保守）セルに組み込み送信する。この番組の受信資格を持つ各受信局では、当該番組用のSKE OAMセルを受信後、予め与えられたこの番組用マスタ鍵で、受信した番組用SKE OAMセルを復号化し、新しいセッション鍵を得る。

【0011】その後、情報送信局は、番組用の鍵変更タイミング通知用のSKC OAMセルを送信すると共に、当該情報送信局における当該番組用のセッション鍵を、SKC OAMセルの送信と同時に、新しいセッション鍵に変更する。また、この番組の受信資格のある全ての受信局で当該番組用のSKC OAMセルを受信すると同時に当該番組用セッション鍵を新しいセッション鍵に変更する。

【0012】

【発明が解決しようとする課題】上述してきたように、従来の片方向通信用暗号化方式は、BS放送用、CS放送用等、複数の受信局で同じ情報を受信する番組毎に異なるセッション鍵及びマスタ鍵を持つ暗号化方式である。

【0013】しかしながら、最近では衛星通信等の片方向通信を用いて1受信局に対してのみ情報を送信したいという需要がある。また、ATM Forumに示されているSKE OAMセル及びSKC OAMセルを用いるセッション鍵の変更法を、受信局毎に異なるセッション鍵を用いるシステムに適用する場合には、SKE OAMセル及びSKC OAMセルは各受信局毎に異なるセルを送信する必要があるため、SKE OAMセル及びSKC OAMセルの送信数は受信局の増加に伴い大きくなり、通信システムの通信帯域に大きな影響を与える。このため、変更用鍵情報及び鍵変更タイミング情報の送信数をできるだけ小さくしたいという課題がある。

【0014】本発明は、上記課題に鑑みてなされたもので、情報送信局で扱えるセッション鍵、マスタ鍵の数を飛躍的に大きくすることにより番組単位のみならず受信局単位の暗号化を可能にすると共に、変更用鍵情報及び鍵変更タイミング情報の送信数を極力、小さくすることのできる暗号化通信方法および暗号化通信システムを提供することを目的とする。

【0015】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項1記載の発明は、情報送信局で暗号化され所定の宛先が付与された伝送情報を送信し、この伝送情報を当該宛先の受信端末で受信し復号化するときの暗号化通信方法であって、情報送信局は、全宛先用のセッション鍵およびマスタ鍵とを記憶し、伝送情報を送信するときには当該伝送情報の宛先に対応するセッション鍵を用いて伝送情報を暗号化して送信し、受信端末は、当該受信端末が受信資格のあるときに割り当てられる宛先用のセッション鍵と宛先用マスタ鍵とを記憶し、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化し、前記セッション鍵を変更する際には、情報送信局は、この情報送信局より送信される変更用鍵情報に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信し、受信端末は、前記変更用鍵情報を受信したときには前記受信端末に記憶されるマスタ鍵を用いて復号し、変更されたセッション鍵を得ることを要旨とする。

【0016】このとき、変更用鍵情報はセッション鍵をマスタ鍵で暗号化したものを記載するものであっても良く、あるいは新規に生成した各宛先用のセッション鍵をマスタ鍵で暗号化して変更用鍵情報としたものであっても良い。さらには各宛先毎に当該宛先用のマスタ鍵で暗号化した複数のセッション鍵を変更用鍵情報に記載するものであっても良く、また複数のセッション鍵をマスタ鍵で暗号化したものであっても良い。

【0017】これにより、請求項1記載の本発明では、セッション鍵の変更の際に、情報送信局より送信する変更用鍵情報を、複数の宛先で同時に受信できる変更用鍵情報配送用の宛先を準備し、各宛先用のマスタ鍵で暗号化したセッション鍵を複数の宛先分送信して変更用鍵情報の数を削減する。

【0018】また請求項2記載の発明は、前記請求項1記載の変更用鍵情報は、各宛先用の鍵変更タイミング情報と共に送信され、当鍵変更タイミング情報に従って前記情報送信局および当該宛先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを要旨とする。

【0019】これにより、請求項2記載の本発明では、セッション鍵の変更の際に、情報送信局より各宛先用の変更用鍵情報を送信し、各変更用鍵情報で送信した鍵の適用は全宛先において1つの宛先用の鍵変更タイミング情報により行い、送信する鍵変更タイミング情報の数を削減する。

【0020】また請求項3記載の発明は、前記請求項1または2記載の情報送信局は、変更用鍵情報及び鍵変更タイミング情報を複数回繰り返して送信することを要旨とする。

【0021】これにより、請求項3記載の本発明では、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【0022】また請求項4記載の発明は、前記請求項1、2または3記載の情報送信局は複数であることを要旨とする。

【0023】これにより、請求項4記載の本発明では、1つの情報送信局にかかる処理負荷が軽減される。

【0024】また請求項5記載の発明は、前記請求項1乃至4のいずれかに記載のセッション鍵の変更は、変更周期が各宛先毎に変えて行われることを要旨とする。

【0025】これにより、請求項5記載の本発明では、必要に応じてセッション鍵の変更周期を、安全性と、変更用鍵情報及び鍵変更タイミング情報の送信によるシステムの送信帯域への影響とのトレードオフにより決定する。

【0026】また請求項6記載の発明は、情報送信局で暗号化され所定の宛先が付与された伝送情報を送信し、この伝送情報を当該宛先の受信端末で受信し復号化するときの暗号化通信システムであって、情報送信局は、全宛先用のセッション鍵およびマスタ鍵とを記憶する記憶手段と、伝送情報を送信するときには当該伝送情報の宛先に対応するセッション鍵を用いて伝送情報を暗号化して送信する伝送情報暗号化手段と、前記セッション鍵を変更する際に変更用鍵情報に複数の宛先に対応するセッション鍵をマスタ鍵で暗号化して送信する変更用鍵情報暗号化手段とを有し、受信端末は、当該受信端末が受信資格のあるときに割り当てられる宛先用のセッション鍵と宛先用マスタ鍵とを記憶する記憶手段と、前記伝送情報を受信したときには当該受信端末に記憶されるセッション鍵を用いて当該伝送情報を復号化する伝送情報復号化手段と、前記セッション鍵を変更する際に前記変更用鍵情報を受信して前記記憶手段に記憶されるマスタ鍵を用いて復号して変更されたセッション鍵を得る変更用鍵情報復号化手段と有することを要旨とする。

【0027】これにより、請求項6記載の本発明では、セッション鍵の変更の際に、情報送信局より送信する変更用鍵情報を、複数の宛先で同時に受信できる変更用鍵情報配送用の宛先を準備し、各宛先用のマスタ鍵で暗号化したセッション鍵を複数の宛先分送信して変更用鍵情報の数を削減する。

【0028】また請求項7記載の発明は、前記請求項6記載の変更用鍵情報は、各宛先用の鍵変更タイミング情報と共に送信され、当鍵変更タイミング情報に従って前記情報送信局および当該宛先の各情報受信局はセッション鍵を新しいセッション鍵に変更することを要旨とする。

【0029】これにより、請求項7記載の本発明では、セッション鍵の変更の際に、情報送信局より各宛先用の変更用鍵情報を送信し、各変更用鍵情報で送信した鍵の適用は全宛先において1つの宛先用の鍵変更タイミング情報により行い、送信する鍵変更タイミング情報の数を削減する。

【0030】また請求項8記載の発明は、前記請求項6または7記載の情報送信局は、変更用鍵情報及び鍵変更タイミング情報を複数回繰り返して送信することを要旨とする。

【0031】これにより、請求項8記載の本発明では、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【0032】また請求項9記載の発明は、前記請求項6、7または8記載の情報送信局は複数であることを要旨とする。

【0033】これにより、請求項9記載の本発明では、1つの情報送信局にかかる処理負荷が軽減される。

【0034】また請求項10記載の発明は、前記請求項6乃至9のいずれかに記載のセッション鍵の変更は、変更周期が各宛先毎に変えて行われることを要旨とする。

【0035】これにより、請求項10記載の本発明では、必要に応じてセッション鍵の変更周期を、安全性と、変更用鍵情報及び鍵変更タイミング情報の送信によ

るシステムの送信帯域への影響とのトレードオフにより決定する。

【0036】すなわち、本発明における暗号化通信方法およびこの方法が適用されるシステムでは、情報送信局は、全宛先用のセッション鍵を宛先順に記憶する記憶手段、全宛先用のマスタ鍵を宛先順に記憶する記憶手段、入力情報を記憶する記憶手段を持ち、情報送信局に送信情報が入力されると、入力情報の宛先を参照し、参照した宛先用のセッション鍵を、前記セッション鍵の記憶手段より高速に検索し、検索されたセッション鍵を用いて前記入力情報を暗号化する暗号手段と、セッション鍵の変更の際に、各宛先で用いる新しいセッション鍵を生成し、当宛先用のマスタ鍵を前記マスタ鍵の記憶手段より高速に検索し、新しいセッション鍵を検索されたマスタ鍵で暗号化した情報を記載した変更用鍵情報を作成、送信する手段と、変更用鍵情報送信後にセッション鍵の変更を行った宛先と新しいセッション鍵の情報より、当該宛先用の鍵変更タイミング情報を作成、送信すると同時に情報送信局内のセッション鍵の記憶手段の当該宛先用のセッション鍵を新しいセッション鍵に変更する手段を備え、受信端末は、受信資格のある宛先用のセッション鍵、受信資格のある宛先用のマスタ鍵及び受信情報を記憶する記憶手段を持ち、受信端末に入力された受信情報の宛先を参照し、参照した宛先用のセッション鍵を受信端末内のセッション鍵の記憶領域より検索し、検索したセッション鍵を用いて受信情報を復号化する復号手段と、受信した変更用鍵情報の宛先を参照し、参照した宛先用のマスタ鍵を受信端末内のマスタ鍵の記憶領域より検索し、検索したマスタ鍵を用いて変更用鍵情報を復号化する復号手段と、鍵変更タイミング情報受信時に、受信した鍵変更タイミング情報の宛先用の新しいセッション鍵を受信端末内にある当該宛先用のセッション鍵記憶領域に書き込む手段とを具備する。

【0037】これにより、セッション鍵の変更の際に、情報送信局より送信する各変更用鍵情報を、複数の宛先で同時に受信できる変更用鍵情報配送用の宛先を準備し、各宛先用のマスタ鍵で暗号化したセッション鍵を複数の宛先分記載、送信することにより送信する変更用鍵情報の数を削減することが可能となる。

【0038】また、セッション鍵の変更の際に、情報送信局より各宛先用の変更用鍵情報を送信し、各変更用鍵情報で送信した鍵の適用は全宛先において1つの全宛先用の鍵変更タイミング情報により行うことにより、送信する鍵変更タイミング情報の数を削減することが可能となる。

【0039】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0040】図1は本発明の一実施の形態に係る暗号化通信方法が適用される暗号化通信システムの情報送信局の要部の構成を示すブロック図であり、図2は同、情報受信局の要部の構成を示すブロック図である。図1に示す情報送信局は鍵管理サーバ11、セッション鍵検索部13およびエンコーダ15により構成され、図2に示す情報受信局はセッション鍵抽出部22、セッション鍵検索部25およびデコーダ26により構成される。

【0041】図1に示す情報送信局内のセッション鍵検索部13では全ての宛先用のセッション鍵を保存しており、鍵管理サーバ11内には、全ての宛先用のセッション鍵配信用のマスタ鍵を保存しているとする。また、図2に示す情報受信局のセッション鍵検索部25では、情報受信局で受信資格を持つ宛先用の全てのセッション鍵を保存し、セッション鍵抽出部22では当受信局で受信資格を持つ宛先用の全てのマスタ鍵を保存しているものとする。なお、これらセッション鍵とマスタ鍵は図示しないハードディスク、光学的記憶媒体等で構成されるデータベースに蓄積、保存される。

【0042】図1において情報受信局では、パケット形式の情報は宛先情報と実際に送信される伝送情報とから構成される。まず、送信される伝送情報（以下、単に送信情報）がエンコーダ15に入力されると、エンコーダ15ではパケットの宛先情報を抽出しセッション鍵検索部13に送信し、当該宛先用のセッション鍵を検索し、エンコーダ13に送出する。エンコーダ13では受け取ったセッション鍵を用いて受信したパケットの宛先情報を除いた送信情報のみを暗号化し、送信する。

【0043】情報受信局においては図2に示すように情報送信局から送信され情報受信局で受信された伝送情報（以下、単に受信情報）がデコーダ26に入力されると受信情報の宛先情報をセッション鍵検索部25に送信し、当該宛先用セッション鍵を検索し、デコーダ26に送信する。デコーダ26では受け取ったセッション鍵を用いて、受信パケットの宛先情報を除いた受信情報のみを復号化し、出力する。

【0044】セッション鍵の変更の際には、図1に示す情報送信局の鍵管理サーバ11で、まず宛先を、セッション鍵の変更を行う宛先とし、新しく生成したセッション鍵を各宛先用のセッション鍵配送用のマスタ鍵で暗号化して変更用鍵情報を生成し、送信する。その後、変更用鍵情報で送信した新しいセッション鍵の適用タイミングを情報受信局に知らせるための、鍵適用タイミング情報を生成し、宛先をセッション鍵変更を行う宛先とし送信する。また、鍵変更タイミング情報の送信とともにセッション鍵検索部13に保存している当宛先用のセッション鍵を新しいセッション鍵に変更する。

【0045】一方、図2に示す情報受信局では、当該情報受信局で受信資格のある宛先用の変更用鍵情報を受信すると、セッション鍵抽出部22で、予め保存している当宛先用のマスタ鍵で変更用鍵情報を復号化し新しいセッション鍵を得る。その後、当宛先用の鍵変更タイミング情報を受信すると同時にセッション鍵検索部25に保存している当宛先用のセッション鍵を新しいセッション鍵に変更する。

【0046】図3は、本発明の暗号化通信方法が適用される暗号化通信システムの1システムを例に、その構成を示すブロック図である。この図3に示す通信システムでは情報サーバ1から送信側システム10を介し受信側システム20へATMセル形式で情報を送信する。ここで送信側システム10の鍵管理サーバ11は、セッション鍵生成部111、マスタ鍵検索部113、SKE OAMセル生成部115およびSKC OAMセル生成部117により構成される。また、受信側システム20は、フィルタ21、セッション鍵抽出部22、マスタ鍵検索部23、新セッション鍵待機部24、セッション鍵検索部25およびデコーダ26により構成される。

【0047】まず、送信側システム10のエンコーダ15は、情報サーバ1から入力したATMセルのヘッダに含まれる宛先情報であるVPI（Virtual Path Identifier）／VCI（Virtual Channel Identifier）をセッション鍵検索部13へ送信する。セッション鍵検索部13は、全VPI／VCI用のセッション鍵を記憶できるように構成されており、入力したVPI／VCI用のセッション鍵を検索し、該当するセッション鍵を出力する。エンコーダ15は、セッション鍵検索部13より入力されたセッション鍵を用いてATMセルのペイロードを暗号化し、ペイロードを暗号化したATMセルを出力する。

【0048】受信側システム20のフィルタ21では、入力したATMセルのヘッダに含まれる宛先情報であるVPI／VCIを参照し、当受信局で受信資格のあるVPI／VCIであるセルのみを出力し、それ以外の入力セルは削除する。デコーダ26では、入力したATMセルのヘッダに含まれる宛先情報であるVPI／VCIをセッション鍵検索部25へ送信する。セッション鍵検索部25は、当該受信局20で受信資格のあるVPI／VCI用の鍵のみを記憶できるように構成されており、入力したVPI／VCI用のセッション鍵を検索し、該当するセッション鍵を出力する。

【0049】デコーダ26は、セッション鍵検索部13より入力されたセッション鍵を用いてATMセルのペイロードを復号化し、ペイロードを復号化したATMセルを出力する。

【0050】セッション鍵の変更は、送信側システム10の鍵管理サーバ11で、セッション鍵の変更を行うVPI／VCIと当VPI／VCIで用いる新しいセッション鍵を生成し新しいセッション鍵を当VPI／VCI用の鍵配送用に用いるマスタ鍵で暗号化し、宛先が当VPI／VCIで、マスタ鍵で暗号化した新しいセッション鍵を含む新しいセッション鍵配送用のSKE OAMセルを作成し出力する。その後、出力したSKE OAMセルと同じ宛先VPI／VCIの鍵変更タイミング通知用のSKC OAMセルを作成し、送信すると同時にセッション鍵検索部13に含まれる当VPI／VCI用のセッション鍵を新しいセッション鍵に変更する。

【0051】受信局側システム20のセッション鍵抽出部22では、SKE OAMセルが入力すると、入力したSKE OAMセルの宛先VPI／VCIをマスタ鍵検索部23に送信する。マスタ鍵検索部23では、当VPI／VCI用のマスタ鍵を検索し、セッション鍵抽出部22へ送信する。セッション鍵抽出部22では、マスタ鍵検索部23より受信したマスタ鍵を用いて、受信したSKE OAMセルに含まれる暗号化されたセッション鍵を復号し、当VPI／VCI用の新しいセッション鍵を抽出し、新セッション鍵待機部24へ送信する。

【0052】新セッション鍵待機部24ではSKC OAMセルの受信と同時に受信したSKC OAMセルの宛先VPI／VCIを参照し、セッション鍵検索部25に送信し、セッション鍵検索部25は記憶される当VPI／VCI用のセッション鍵を新しいセッション鍵に変更する。

【0053】図4に情報送信局及び情報受信局A、情報受信局B、情報受信局Cを持つシステムにおけるセッション鍵の変更法を用いる場合のタイムチャートを示す。

【0054】まず、情報送信局で情報受信局A宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Aのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局A宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Aのみこの鍵変更タイミング情報を受信し、情報受信局Aのセッション鍵の変更を完了する。

【0055】次に、情報送信局で情報受信局B宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Bのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局B宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Bのみこの鍵変更タイミング情報を受信し、情報受信局Bのセッション鍵の変更を完了する。

【0056】最後に、情報送信局で情報受信局C宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Cのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局C宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Cのみこの鍵変更タイミング情報を受信し、情報受信局Cのセッション鍵の変更を完了する。

【0057】図5に各変更用鍵情報に各宛先用のマスタ鍵で暗号化したセッション鍵を、複数の宛先分記載、送信する場合の、変更用鍵情報のパケット構成の例を示す。図5に示すパケットでは、情報受信局A、情報受信局B、情報受信局C用の変更用鍵情報（各宛先用のマス

タ鍵で暗号化したセッション鍵）を記載し、宛先として情報受信局Ａ～情報受信局Ｃへの同報用の宛先を用いる。

【００５８】この図５に示す変更用鍵情報を用いて、情報送信局、情報受信局Ａ、情報受信局Ｂ、情報受信局Ｃを持つシステムにおいて、セッション鍵の変更を行う際のタイムチャートを図６に示す。

【００５９】図６を参照するに、まず情報送信局より、図５に示すＡ，Ｂ，Ｃ宛の変更用鍵情報を送信する。各情報受信局Ａ～Ｃでは、予めこの変更用鍵情報における各宛先用の変更用鍵情報の記載領域を認識しており、それぞれ受信した変更用鍵情報の該当する領域に記載されている情報を、各情報受信局において予め保存している各宛先用のマスタ鍵で復号化することにより、新しいセッション鍵を得る。

【００６０】次に情報送信局で情報受信局Ａ宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Ａのみこの鍵変更タイミング情報を受信し、情報受信局Ａのセッション鍵の変更を完了する。

【００６１】次に、情報送信局で情報受信局Ｂ宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Ｂのみこの鍵変更タイミング情報を受信し、情報受信局Ｂのセッション鍵の変更を完了する。

【００６２】次に、情報送信局で情報受信局Ｃ宛の鍵変更タイミング情報を作成、送信し、各情報受信局においては、情報受信局Ｃのみこの鍵変更タイミング情報を受信し、情報受信局Ｃのセッション鍵の変更を完了する。

【００６３】図７に１つの鍵変更タイミング情報を複数の情報受信局用として用いる場合の鍵変更タイミング情報のパケット構成の一例を示す。図７に示すパケットでは宛先として情報受信局Ａ～情報受信局Ｃへの同報用の宛先を用いる。この図７に示す鍵変更タイミング情報パケットを用いて、情報送信局、情報受信局Ａ、情報受信局Ｂ、情報受信局Ｃを持つシステムにおいて、セッション鍵の変更を行う際のタイムチャートを図８に示す。

【００６４】まず、情報送信局で情報受信局Ａ宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Ａのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局Ｂ宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Ｂのみこの変更用鍵情報を受信する。次に、情報送信局で情報受信局Ｃ宛の変更用鍵情報を作成、送信し、各情報受信局においては、情報受信局Ｃのみこの変更用鍵情報を受信する。最後に情報送信局で図７に示す鍵変更タイミング情報を作成、送信し、各情報受信局ではこの鍵変更タイミング情報を受信し、セッション鍵の変更を完了する。

【００６５】次に図９及び図１０に示すタイムチャートを参照して、変更用鍵情報に記載のセッション鍵を複数回だけ同じセッション鍵を変更用鍵情報として送信する方法の有効性について説明する。図９に、情報送信局より情報受信局Ａへ、Ａ宛の変更用鍵情報及びＡ宛の鍵変更タイミング情報を２回ずつ送信し、情報受信局Ａにおいて１回目に送信されたＡ宛の変更用鍵情報を情報受信局Ａで受信できなかった場合のタイムチャートを示している。この場合、１回目に送信されるＡ宛の変更用鍵情報は情報受信局Ａにおいて無効とされ、２回目に送信されるＡ宛の変更用鍵情報及びＡ宛の鍵変更タイミング情報によりセッション鍵の変更が完了する。

【００６６】図１０に、情報送信局より情報受信局Ａへ、Ａ宛の変更用鍵情報及びＡ宛の鍵変更タイミング情報を２回ずつ送信し、情報受信局Ａにおいて１回目に送信されたＡ宛の鍵変更タイミング情報を情報受信局Ａで受信できなかった場合のタイムチャートを示す。この場合、２回目に送信されるＡ宛の変更用鍵情報は無効とし、１回目に送信されたＡ宛の変更用鍵情報と２回目に送信される鍵変更タイミング情報によりセッション鍵の変更が完了する。

【００６７】図１１に本発明を応用した、情報サーバ、情報送信局、情報受信局ａ、情報受信局ｂ、情報受信局ｃ、情報受信局ｄを持つシステムの構成の概要を示す。図１１の情報送信局においては、情報サーバより入力され、情報受信局ａ～情報受信局ｄへ送信される全ての情報の、暗号化処理を行うことになる。

【００６８】これに対して、応用例として、図１２に情報サーバ、情報送信局Ａ、情報送信局Ｂ、情報受信局ａ、情報受信局ｂ、情報受信局ｃ、情報受信局ｄを持つシステムの構成の概要を示す。図１２の情報送信局Ａにおいては、情報サーバより、情報受信局ａ及び情報受信局ｂ宛に送信される情報の暗号化処理を行い、情報送信局Ｂにおいては、情報サーバより、情報受信局ｃ及び情報受信局ｄ宛に送信される情報の暗号化処理を行う。このため、図１２の情報受信局Ａ及び情報受信局Ｂでは、図１１の情報受信局での処理が分散されることになる。

【００６９】図１３にセッション鍵の変更周期を各宛先毎に変えて行う暗号化通信方法を実現するための情報送信局内の鍵管理サーバの構成の一例を示す。図１３に示す鍵管理サーバは、第１の鍵変更タイミング管理部１１０Ａと第２の鍵変更タイミング管理部１１０Ｂが接続されるセッション鍵生成部１１１と、このセッション鍵生成部１１１に順次接続されるマスタ鍵検索部１１３、変更用鍵情報生成部１１４および鍵変更タイミング情報生成部１１６により構成される。

【００７０】第１の鍵変更タイミング管理部１１０Ａでは、各受信局宛情報用の宛先のセッション鍵の変更タイミング（変更用鍵情報及び鍵変更タイミング情報の送信間隔）を管理し、例えば１０秒毎に第１の鍵変更タイミング管理部１１０Ａで管理する全ての宛先のセッション鍵の変更を行う。

【００７１】また、第２の鍵変更管理部１１０Ｂでは複数の受信局宛の、番組等の情報用の宛先のセッション鍵の変更タイミング（変更用鍵情報及び鍵変更タイミング情報の送信間隔）を管理し、例えば５秒毎に第２の鍵変更管理部１１０Ｂで管理する全ての宛先のセッション鍵の変更を行う。

【００７２】これにより、各情報受信局では、各情報受信局用の変更用鍵情報及び鍵変更タイミング情報は１０秒毎に受信されることにより、各情報受信局宛情報用のセッション鍵は１０秒毎に変更される。また、複数の受信局宛の、番組等の情報用の変更用鍵情報及び鍵変更タイミング情報は５秒毎に受信されることにより、複数の受信局宛の、番組等の情報の宛先用のセッション鍵は５秒毎に変更される。このように目的に合わせてセッション鍵の変更周期を各宛先毎に変えることができる。

【００７３】図１４に図１３に示す情報送信局内の鍵管理サーバを持つことにより、情報受信局Ａ及び情報受信局Ｂ用の宛先のセッション鍵の変更を１０秒毎に、情報受信局Ａ及び情報受信局Ｂで受信資格を持つ番組１の宛先用のセッション鍵の変更を５秒毎に行うときの情報送信局と各情報受信局間のタイムチャートを示す。

【００７４】図１４を参照するに、番組１用の変更用鍵情報及び鍵変更タイミング情報の送信、Ａ宛の変更用鍵情報及び鍵変更タイミング情報の送信、Ｂ宛の変更用鍵情報及び鍵変更タイミング情報の送信をまず行う。

【００７５】そして約５秒後に番組１用の変更用鍵情報及び鍵変更タイミング情報の送信、更に約５秒後に番組１用の変更用鍵情報及び鍵変更タイミング情報の送信、Ａ宛の変更用鍵情報及び鍵変更タイミング情報の送信、Ｂ宛の変更用鍵情報及び鍵変更タイミング情報の送信をまず行う。このように情報送信局内で宛先毎にセッション鍵の変更周期を変更することができる。

【００７６】尚、上記の実施形態ではＡＴＭに適用した場合を例にとって説明したが、本発明はこれに限定されること無く、いかなる形式のパケットを暗号化する暗号化通信システムにおいても、またいかなる暗号化アルゴリズムを用いる暗号化通信システムにおいても、またいかなるセッション鍵の変更周期をもつ暗号化通信システムにおいても適用できる。

【００７７】

【発明の効果】上述したように本発明の請求項１および６に記載の暗号化通信方法およびシステムによれば、各変更用鍵情報に各宛先用のマスタ鍵で暗号化したセッション鍵を複数の宛先分記載、送信できるので、各宛先毎に異なる変更用鍵情報を作成、送信する場合に比べ、送信する変更用鍵情報の個数を減らすことができる。

【００７８】また、請求項２および７に記載の暗号化通信方法およびシステムを用いると、情報送信局より各宛先毎に変更用鍵情報を送信し、送信した各変更用鍵情報に記載のセッション鍵の適用を全宛先用の鍵適用タイミング情報１つで行うため、各宛先毎に異なる鍵適用タイミング情報を送信する場合に比べ送信する鍵変更タイミング情報の個数を減らすことができる。

【００７９】また、請求項３および８に記載の暗号化通信方法およびシステムを用いると、情報送信局より各情報受信局へ、変更用鍵情報及び鍵変更タイミング情報を複数回送信することから、各情報受信局において、変更用鍵情報及び鍵変更タイミング情報の受信失敗の際に、再送される変更用鍵情報及び鍵変更タイミング情報によりセッション鍵の変更を完了せしめることができるため、各情報受信局においてセッション鍵の変更を失敗する確率が小さくなる。

【００８０】請求項４および９に記載の暗号化通信方法およびシステムを用いると、情報送信局が複数であることから、１つの情報送信局にかかる処理負荷が軽減される。

【００８１】請求項５および１０に記載の暗号化通信方法およびシステムを用いると、セッション鍵の変更周期を宛先毎に変えることができるため、必要に応じてセッション鍵の変更周期を、安全性と、変更用鍵情報及び鍵変更タイミング情報の送信によるシステムの送信帯域への影響とのトレードオフにより決定することができる。

【図面の簡単な説明】

【図１】本発明に係る通信システムにおける情報送信局の一実施形態の概略の構成を示すブロック図である。

【図２】本発明に係る通信システムにおける情報受信局の一実施形態の概略の構成を示すブロック図である。

【図３】本発明に係る通信システムのシステム全体の概略の構成を示すブロック図である。

【図４】セッション鍵変更法を用いる場合の情報送信局と情報受信局との間のタイムチャートである。

【図５】図１に示す情報送信局から送信される変更用鍵情報の構成例を示す図である。

【図６】図３に示す通信システムで用いられるセッション鍵変更法における情報送信局と情報受信局間のタイムチャートである。

【図７】他の鍵変更タイミング情報の構成例を示す図である。

【図８】他の通信システムで用いられるセッション鍵変更法における情報送信局と情報受信局間のタイムチャートである。

【図９】１回目に送信された変更用鍵情報が情報受信局で正しく受信できなかった場合のタイムチャートである。

【図１０】１回目に送信された鍵変更タイミング情報が情報受信局に正しく受信できなかった場合のタイムチャートである。

【図１１】本発明が適用される一般的な通信システムの構成を示すブロック図である。

【図１２】他の通信システムの構成を示すブロック図である。

【図１３】宛先毎にセッション鍵の変更周期を変える方

15　16

法を実現するための情報送信局内の鍵管理サーバの構成を示すブロック図である。

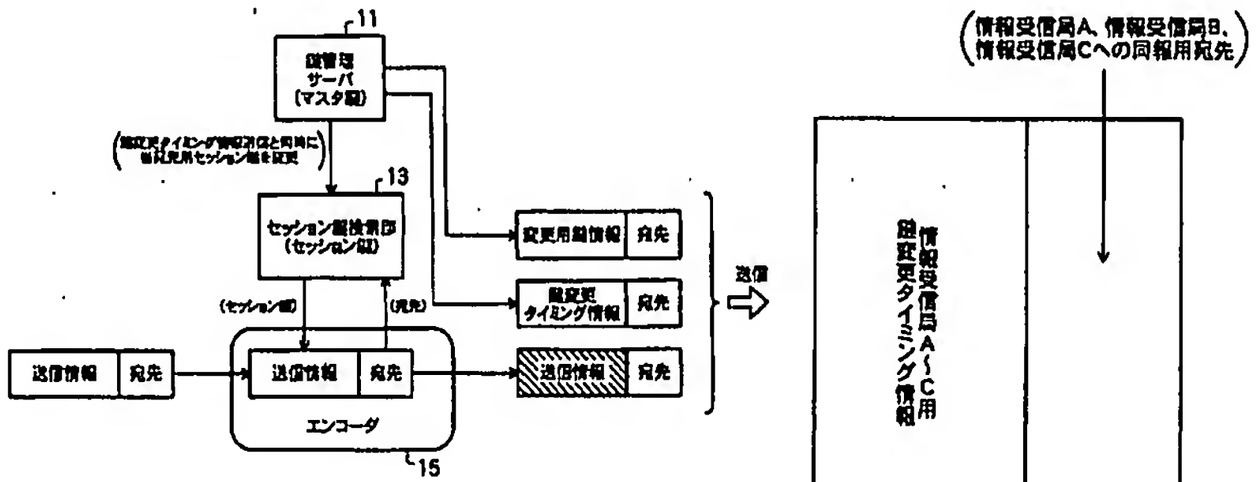
【図１４】宛先毎にセッション鍵の変更周期を変える方法を適用した情報送信局と情報受信局間のタイムチャートである。

【図１５】衛星放送で用いられるスクランブル方法の３重鍵暗号の概要を示す図である。

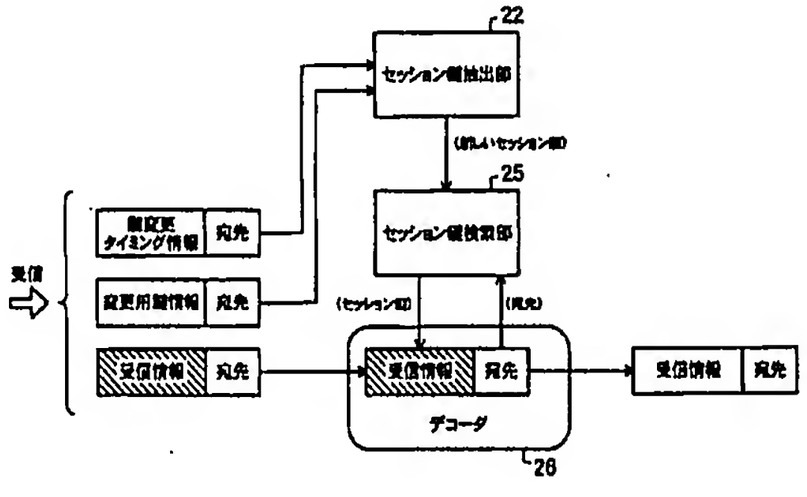
【符号の説明】

１　情報サーバ
１０　送信側システム
１１　鍵管理サーバ
１３　セッション鍵検索部
１５　エンコーダ
２０　受信側システム
２１　フィルタ
２２　セッション鍵抽出部
２３　マスタ鍵検索部
２４　新セッション鍵待機部
２５　セッション鍵検索部
２６　デコーダ
１１１　セッション鍵生成部
１１３　マスタ鍵検索部
１１５　ＳＫＥ　ＯＡＭセル生成部
１１７　ＳＫＣ　ＯＡＭセル生成部

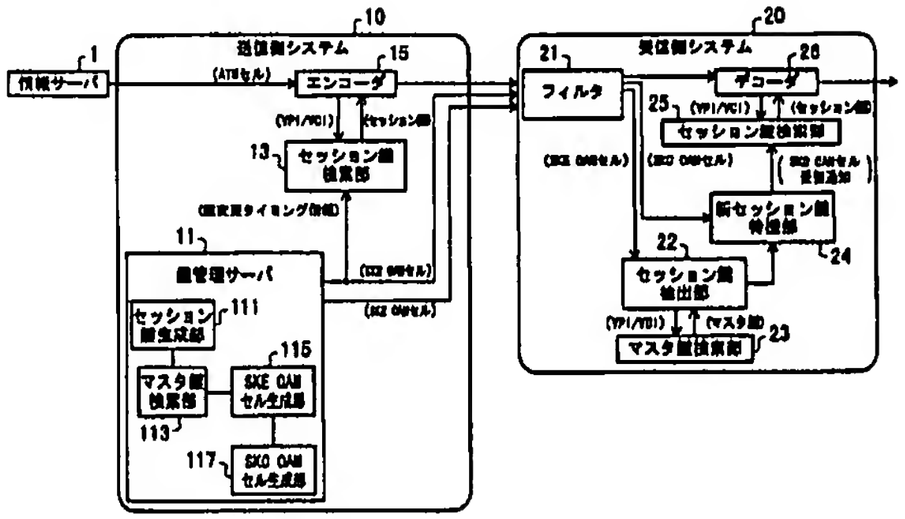
【図１】



【図２】

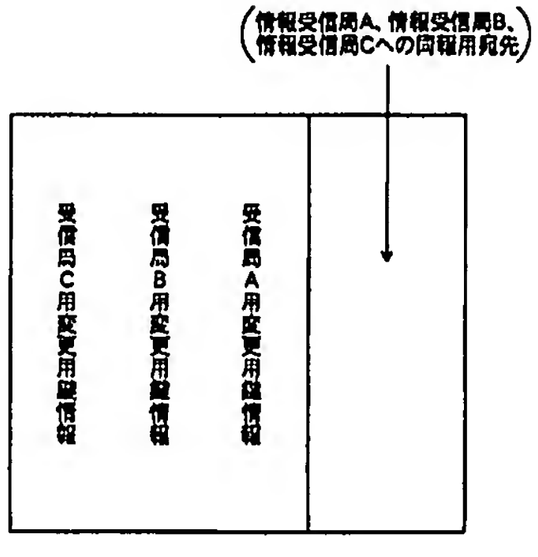


【図３】

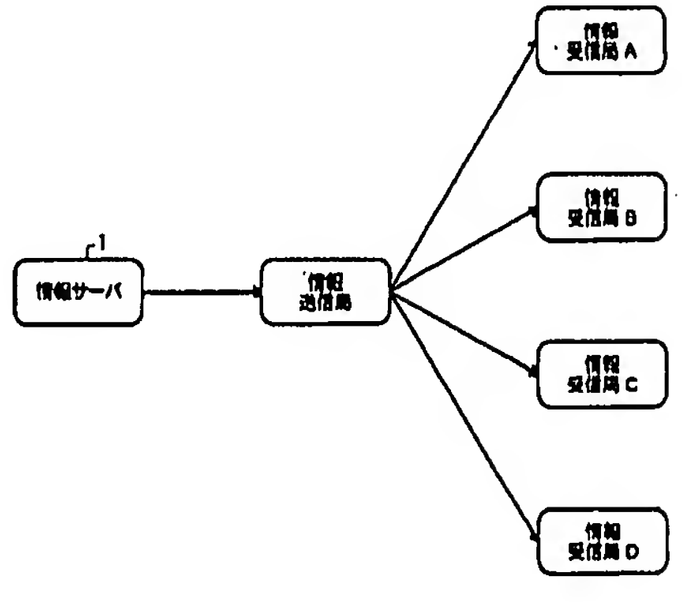


【図４】

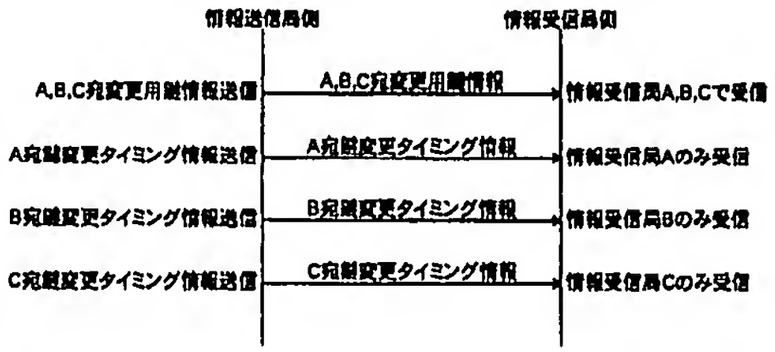
【図５】



【図１１】

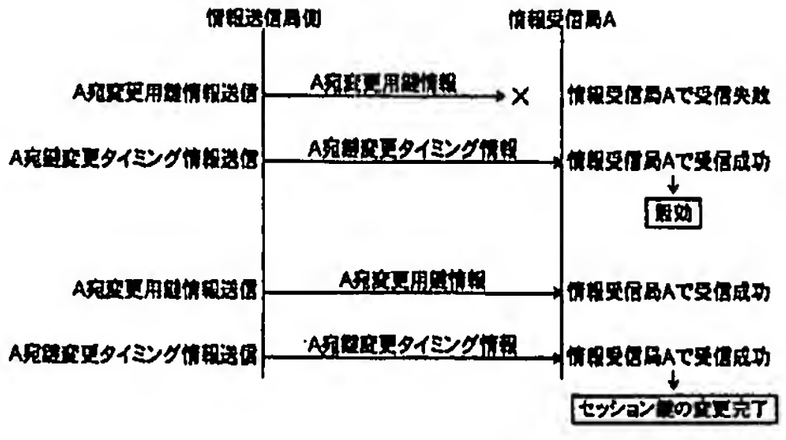


【図６】

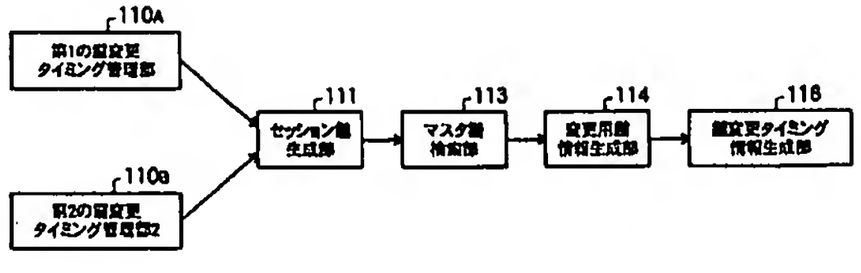


【図８】

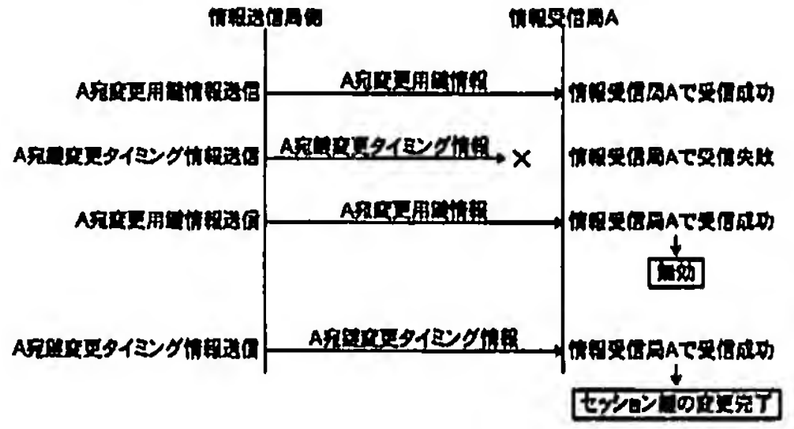
【図９】



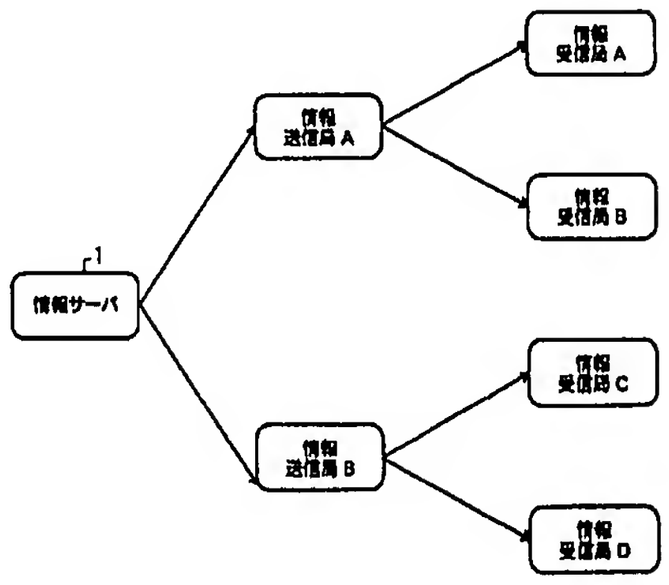
【図１３】



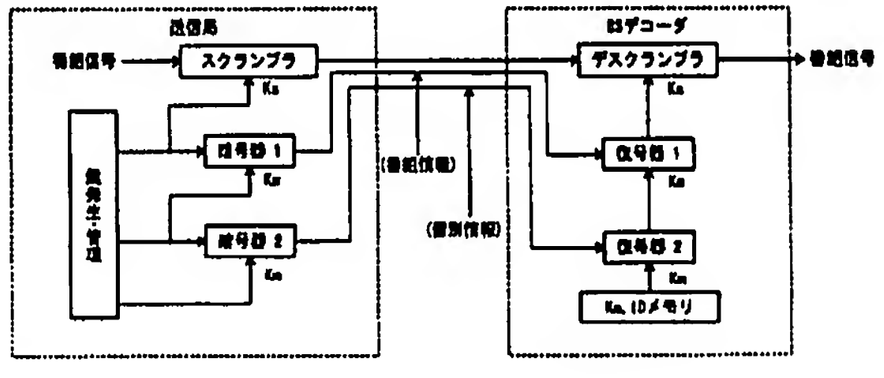
【図１０】



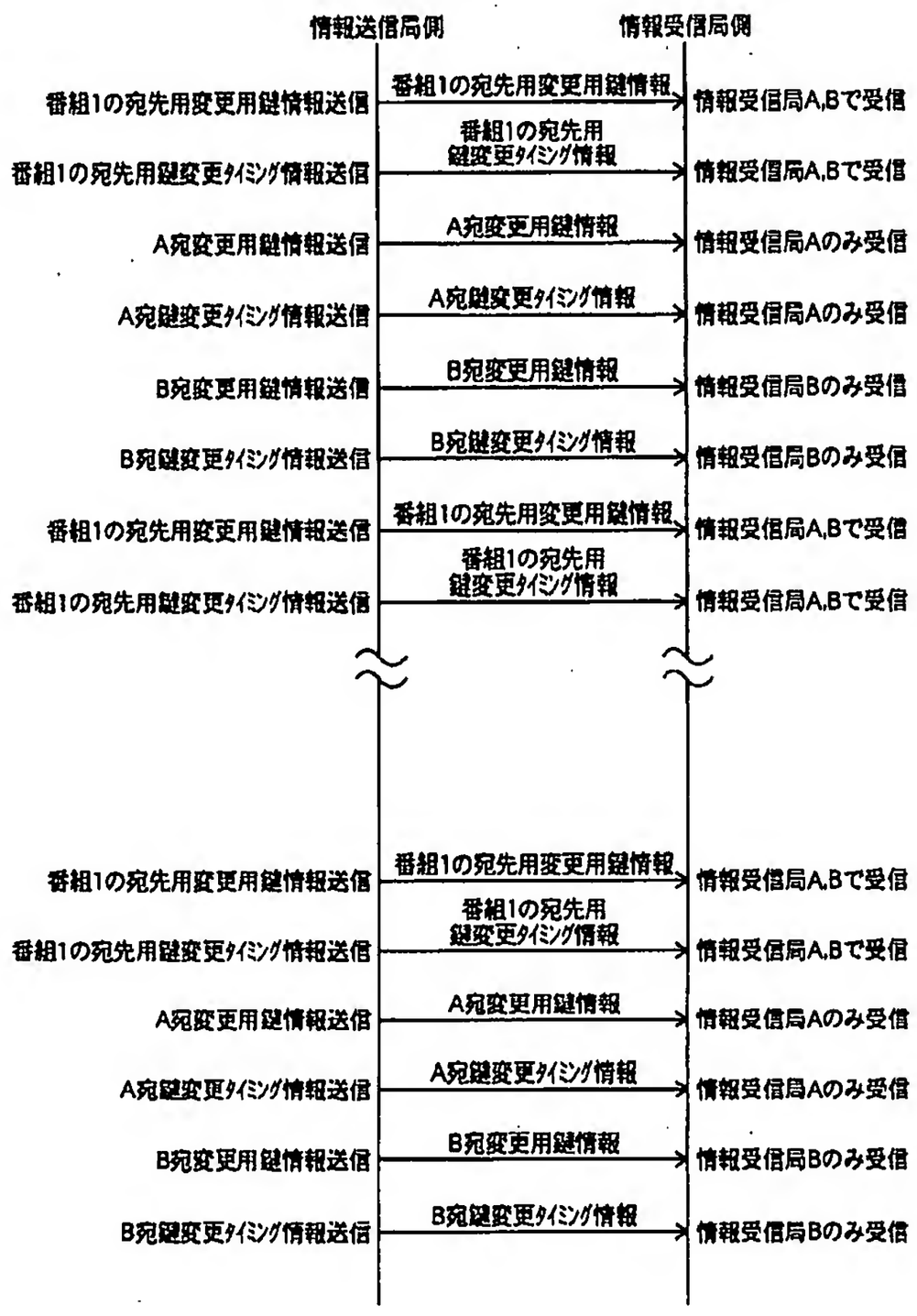
【図１２】



【図１５】



【図１４】



フロントページの続き

(72)発明者　荒木　克彦
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内